Aqil Azmi, PhD. at 1/19/2021 8:00 AM

Def. Proposition: any statement that is either true or false, but not both.

Ex. "Today is sunny." } Propositions
$1+3=10$
$x+1=10$
"what is your name?" } not proposition

compound proposition: new proposition using logical operators

Logical operators: AND, OR, XOR, Implication,...
$p \wedge q$, $p \vee q$, $p \oplus q$, $p \to q$

Truth table: display relationship between truth values of propositions,

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$
T	T	T	T	F	T
T	F	F	T	T	F
F	T	F	T	T	T
F	F	F	F	F	T

Ex. $(p \to q) \wedge p$ $\quad$ $p \to (q \wedge p)$

- converse of $p \to q$ is $q \to p$

- Contrapositive of $p \to q$ is $\neg q \to \neg p$

- Biconditional $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$

Def. Tautology: a compound proposition that is always true.

Def. Contradiction: a compound proposition that is always false.

$p \wedge (\neg p)$ Contradiction

$p \vee (\neg p)$ tautology

- Logical equivalences: $p \Leftrightarrow q$

Ex. $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

Logical equivalences

Identity law

$p \wedge T \Leftrightarrow p$

$p \vee F \Leftrightarrow p$

Domination law

$p \vee T \Leftrightarrow T$

$p \wedge F \Leftrightarrow F$

Idempotent law

$p \wedge p \Leftrightarrow p$

$p \vee p \Leftrightarrow p$

Double negation

$\neg(\neg p) \Leftrightarrow p$

Commutative

$p \wedge q \Leftrightarrow q \wedge p$

$p \vee q \Leftrightarrow q \vee p$

Associative

$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

Distributive

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

DeMorgan

$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

Misc

$p \wedge \neg p \Leftrightarrow F$

$p \vee \neg p \Leftrightarrow T$

$(p \rightarrow q) \Leftrightarrow \neg p \vee q$

Aqil at 1/21/2021 8:01 AM

Ex. Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

$$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$$
$$\Leftrightarrow \neg p \wedge (p \vee \neg q)$$
$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q)$$
$$\Leftrightarrow F \vee (\neg p \wedge \neg q)$$
$$\Leftrightarrow \neg p \wedge \neg q$$

Ex. Determine if $\neg(p \wedge (p \to q)) \to \neg q$ is a tautology?

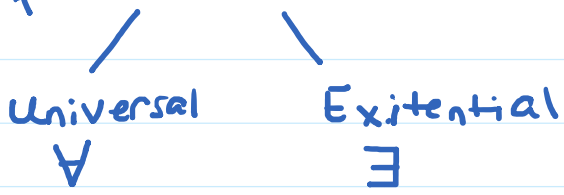
$$\neg(p \wedge (p \to q)) \to \neg q \Leftrightarrow (p \wedge (p \to q)) \vee \neg q$$
$$\Leftrightarrow \neg q \vee (p \wedge (p \to q))$$
$$\Leftrightarrow (\neg q \vee p) \wedge (\neg q \vee (p \to q))$$
$$\Leftrightarrow (\neg q \vee p) \wedge (\neg q \vee (\neg p \vee q))$$
$$\Leftrightarrow (\neg q \vee p) \wedge (T \vee \neg p)$$
$$\Leftrightarrow \neg q \vee p$$
$$\Leftrightarrow q \to p \quad \not\Leftrightarrow T$$

* Consider the statement "$x > 5$" not proposition
* we define proposition function $P(x) =$ "$x > 5$".
* $P(1)$ False
  $P(100)$ True

* We can define proposition function
$Q(x, y)$ = "$x + 2 = y$"

* $Q(1, 1)$ False
$Q(5, 7)$ True.

* We can assign values to the variables using quantifiers



Def. The universal quantification of $P(x)$ is the proposition "$P(x)$ is true for all values of x in a particular domain (universe of discourse).

$\forall x\ P(x)$

universe of discourse = set of all values x takes

* Assume universe of discourse is $\{x_1, x_2, \ldots, x_n\}$ then,

$$\forall x\ P(x) = P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

$$= \bigwedge_{i=1}^{n} P(x_i)$$

Ex Let $P(x)$ = "$x+5 > 0$"

Find $\forall x\ P(x)$ if universe of discourse is $\mathbb{R}$ then $\forall x\ P(x)$ is False.

And if universe of discourse is $\mathbb{Z}^+$ then $\forall x\ P(x)$ is True.

Def. The existential quantification of $P(x)$ is the proposition "There exist an element x in the universe of discourse $\ni$ $P(x)$ is true"

$$\exists x\ P(x)$$

* Assume if universe of discourse is the set $\{x_1, x_2, \ldots, x_n\}$ then

$$\exists x\ P(x) = P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

$$= \bigvee_{i=1}^{n} P(x_i)$$

Ex. Let $Q(x)$ = "$x > 5$"

if Universe of discourse is $\mathbb{R}$ then $\exists x\ Q(x)$ is True.

if universe of discourse is $\mathbb{Z}^-$ then $\exists x\ Q(x)$ is false

Expressing English statements using proposition functions

Let $F(x,y)$ = "y is the father of x"

* Express "Ali is father of Bilal"

$F(Bilal, Ali)$

* Express "Everyone has a father"

$\forall x \exists y \; F(x,y)$ universe of discourse is all humans

* Express "Everyone has a single father"

$\forall x \exists y \forall z \; F(x,y) \wedge ((z \neq y) \rightarrow \neg F(x,z))$

* Express "Everyone has a father and a mother"

Let $M(x,y)$ = "y is the mother of x"

$\forall x \exists y \exists z \; F(x,y) \wedge M(x,z)$

Order of quantifiers is important.

* $\forall x \forall y \; A(x,y) \equiv \forall y \forall x \; A(x,y)$

$\exists x \exists y A(x,y) \equiv \exists y \exists x A(x,y)$

* Let $Q(x,y)$ = "$x+y=0$"

$\underbrace{\forall x \exists y Q(x,y)}_{\text{True}}$ assume universe of discourse is $\mathbb{Z}$

$\underbrace{\exists y \forall x Q(x,y)}_{\text{False}}$ (idea: pick any y, there is only one $x \ni x+y=0$, but there is no single $y \ni x+y=0$)

$\forall x \exists y \not\equiv \exists y \forall x$

* $\neg(\forall x P(x)) \Leftrightarrow \exists x(\neg P(x))$

$\neg(\exists x P(x)) \Leftrightarrow \forall x(\neg P(x))$

Ex Let $P(x)$ = "x knows Arabic"

$\forall x P(x)$ = "all students know Arabic"

↑ universe of discourse is all students in the classroom

$\neg \forall x P(x)$ = "not all students know Arabic"

$\exists x \neg P(x)$ = "there is a student does not know Arabic"

Sets: a collection of objects

Ex. $A = \{1, \text{car}, \square\} = \{\text{car}, 1, \square\}$

↑ element of the set. $\text{car} \in A$

$3 \notin A$

$P = \{2, 3, 5, 7, 11, 13\}$

$= \{x \mid x \text{ is prime} < 15\}$

* Two sets are equal if they have the same elements

* Empty set is a set with no elements $\emptyset$
* Sets A, B

$A \subset B$ A is proper subset of B

$A \subseteq B$ A is subset of B

↑

each element in A is in set B

$\forall a \, (a \in A \rightarrow a \in B)$

* To show set $A = B \Rightarrow$ ① show $A \subseteq B$

② " $B \subseteq A$

Ex Set $Q = \{2,3,5,7\} \subset P = \{2,3,5,7,11,13\}$

NOTE: $\phi \subseteq$ of any set

$\phi \subseteq Q$, $\phi \notin Q$

* We can define set containing other sets

$A = \{1, 2, \{3,4\}, \{5,6,7\}, \phi\}$

↑ ↑ ↑ ↑ ↑ 5 elements

Cardinality of set A $= |A| = 5$

$\phi \in A$ $\quad \phi \subset A$

$1 \in A$ $\quad 1 \notin A$

$3 \notin A$ $\quad 3 \notin A$

$\{3,4\} \in A$ $\quad \{1, \{3,4\}\} \subset A$

$\{\{3,4\}\} \subset A$

$\{\phi\} \subset A$

$\{3\} \notin A$

* Powerset : Set of all subsets of a Set

Ex Set $A = \{1,2,a\}$

$P(A) = \{\phi, \{1\}, \{2\}, \{a\}, \{1,2\}, \{1,a\}, \{2,a\}, \{1,2,a\}\}$

$|A|$

$$|P(A)| = 2^{|A|}$$

Ex. $P(\emptyset) = \{\emptyset\} = \{\{\}\}$ $\quad \emptyset = \{\}$

$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

* Sets A, B

Cartesian product $A \times B = \{\underbrace{(a,b)}_{\text{pair}} \mid a \in A \wedge b \in B\}$

$$A_1 \times A_2 \times A_3 = \{\underbrace{(x,y,z)}_{\text{3-tuple}} \mid x \in A_1 \wedge y \in A_2 \wedge z \in A_3\}$$

Ex. $A = \{1,2,3\}$, $B = \{x,y\}$

$A \times B = \{(1,x), (1,y), (2,x), (2,y), (3,x), (3,y)\}$

$1 \notin A \times B$

$(1,x) \in A \times B$ $\quad (1,x) \notin A \times B$

$\{(1,x)\} \subset A \times B$

$$|A \times B| = |A| \cdot |B|$$

$A \times \phi = \phi$

Set Operations

- Complement: $\bar{A} = \{x \mid x \notin A\}$
- Difference: $A - B = \{x \mid x \in A \wedge x \notin B\}$
- Intersection: $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- Union: $A \cup B = \{x \mid x \in A \vee x \in B\}$

* if $A \cap B = \phi$ we say they are disjoint sets

Set Identities

1. Identity law: $A \cup \phi = A$, $A \cap U = A$ (Universal set)
2. Domination law: $A \cap \phi = \phi$, $A \cup U = U$
3. Idempotent: $A \cup A = A \cap A = A$
4. Double complement: $\bar{\bar{A}} = A$
5. Commutative law: $A \cup B = B \cup A$, $A \cap B = B \cap A$
6. Associative law: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$

⑦ Distributive law $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

⑧ De Morgan Law $\overline{A \cup B} = \bar{A} \cap \bar{B}$

$\overline{A \cap B} = \bar{A} \cup \bar{B}$

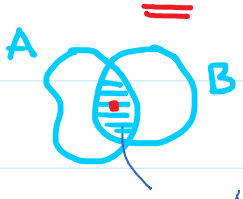
Ex Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

① Show $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$

Let $x \in \overline{A \cap B}$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \notin A$ or $x \notin B$



$x \in A \cap B$

if $x \notin A \cap B$

$\Rightarrow x \notin A \vee x \notin B$

$\Rightarrow x \in \bar{A}$ or $x \in \bar{B}$

$\Rightarrow x \in \bar{A} \cup \bar{B}$

② Show $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

let $x \in \bar{A} \cup \bar{B}$

$\Rightarrow x \in \bar{A}$ or $x \in \bar{B}$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \in \overline{A \cap B}$

We can prove above using set building notation

$\overline{A \cap B} = \{x \mid x \notin A \cap B\}$

$= \{x \mid \neg(x \in A \cap B)\}$

$$= \{x \mid \neg(x \in A \wedge x \in B)\}$$

$$= \{x \mid x \notin A \vee x \notin B\}$$

$$= \{x \mid x \in \bar{A} \vee x \in \bar{B}\}$$

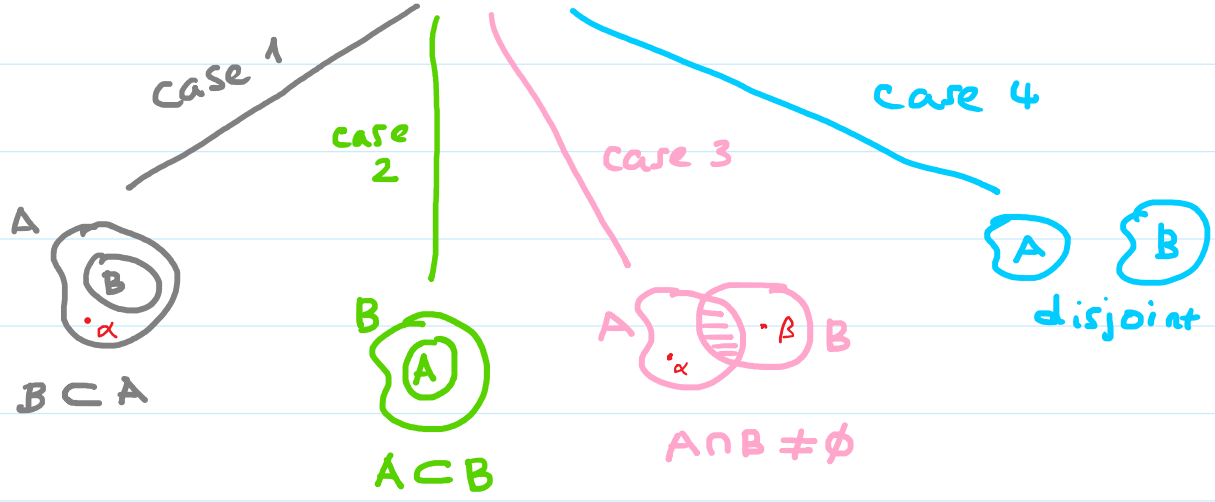
$$= \{x \mid x \in \bar{A} \cup \bar{B}\}$$

* $A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$

* $A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$

Problem: Given sets A, B, C

if $A \cup C = B \cup C$ and $A \cap C = B \cap C$ } is it possible that $A \neq B$?



Aqil at 2/2/2021 8:26 AM

case #1. Let $A = B \cup \{\alpha\} \ni \alpha \notin B$.

Then $A \cup C = B \cup C \Rightarrow \alpha \in C$ otherwise no equality.

$A \cap C = B \cap C \Rightarrow \alpha \notin C$ " " "

$\therefore B \not\subset A$.

case #2. Assume $A \subset B$. Same as above, i.e $A \not\subset B$.

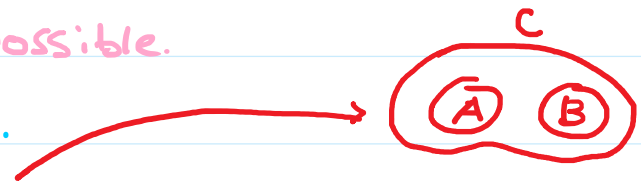
case #3. Let $A = \{\square, \alpha\}$, and $B = \{\square, \beta\}$ such that $\square$ is common to A and B, $\alpha \notin B$, and $\beta \notin A$

Then $A \cup C = B \cup C \Rightarrow \alpha \in C$ and $\beta \in C$

$A \cap C = B \cap C \Rightarrow \alpha \notin C$ and $\beta \notin C$

$\therefore$ this scenario not possible.

case #4. A, B disjoint.



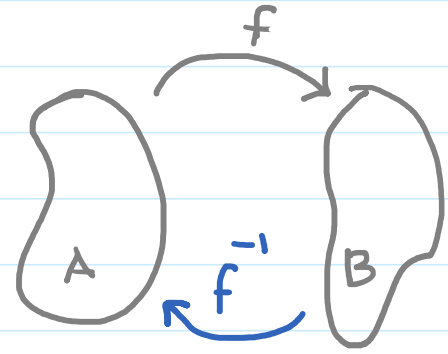
Then $A \cup C = B \cup C \Rightarrow A \subset C$ and $B \subset C$

$A \cap C = B \cap C \Rightarrow A \not\subset C$ and $B \not\subset C$

Therefore, $A \neq B$ fails and thus $A = B$.

Functions

Def: Sets A, B. The function from A to B is an assignment of one element of B to each element of A.



domain of f

co domain of f

$f: A \to B$

$f(a) = b$

image of a under f

pre-image of b under f

* Range of f: set of all images of A, $\{f(a) \mid \forall a \in A\}$

* Types of functions

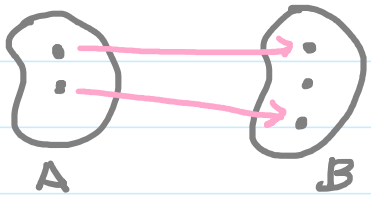
1-1: Each $b \in B$ receive <u>at most</u> 1 arrow

Onto: " $b \in B$ " <u>at least</u> 1 "

1-1 corr: " $b \in B$ " exactly 1 "

Neither: none of the above

1-1:

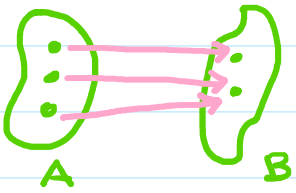


$f(a) = f(b) \Rightarrow a = b$

$a \neq b \Rightarrow f(a) \neq f(b)$

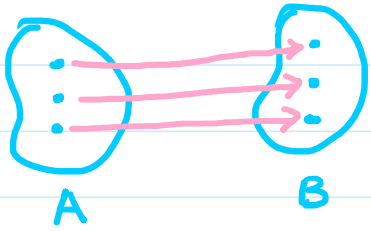
$|A| \leq |B|$

Onto:



$|A| \geq |B|$

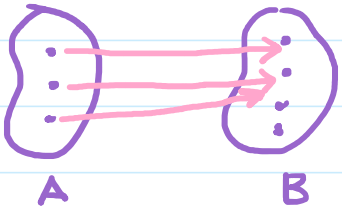
1-1 Correspondance:



= 1-1 and Onto

$|A| = |B|$

Neither:



NOTE: When f is 1-1 or onto some elements do not have f^{-1}!
Only when f is 1-1 correspondance do we have inverse of each element.

Def. Let $f: A \to B$ and $g: B \to C$, then the composition of g and f is,

$$(g \circ f)(a) = g(f(a))$$

No $f \circ g$.

Ex. Assume $f: \mathbb{R} \to \mathbb{R}$, $g: \mathbb{R} \to \mathbb{R}$.

Let $f(x) = 2x + 3$

$g(x) = 3x - 5$

$$(f \circ g)(x) = f(g(x))$$
$$= f(3x - 5)$$
$$= 2(3x - 5) + 3$$
$$= 6x - 7$$

$$(g \circ f)(x) = g(f(x))$$
$$= g(2x + 3)$$
$$= 3(2x + 3) - 5$$
$$= 6x + 4$$

Sequences

Def. Sequence is a function $f: A \to S \Rightarrow A \subset \mathbb{Z}$.

Usually A is the set $\{0, 1, 2, \ldots\}$ or $\{1, 2, 3, \ldots\}$.

* a_n denotes image of integer n.
* a_n is called term of the sequence.

(n ↑ index)

Ex. The sequence $\{a_n\} \ni a_n = 1/n$ is the sequence

$\{1, 1/2, 1/3, \ldots\}$

Ex. The sequence $\{b_n\} \ni b_n = 2n$ is the sequence

$\{0, 2, 4, 6, \ldots\}$

b_0 b_1 b_2 b_3

Arithmetic sequence $a_n - a_{n-1} =$ Constant

Geometric " $\frac{a_n}{a_{n-1}} =$ constant.

Ex. Consider the sequence $\{6, 11, 16, 21, \ldots\}$.

What is the next term? 26

Ex. Let sequence $a_1 = \{7, 13, 19, 25 \}$

(6 6 6)

Ex. Let sequence $a_n\big|_{n\geq 1} = \{7, 13, 19, 25, \ldots\}$

a_1 a_2 a_3

Find a_{100} ?

Formula for arithmetic sequence is

$a_n = a_1 + d(n-1)$ $\quad n \geq 1$

Above $a_1 = 7$, $d = 6$

Then $a_n = 7 + 6(n-1)$

$= 6n + 1$

So, $a_{100} = 6 \times 100 + 1 = 601$

Ex. Consider the sequence $a_{50} = 102$, $a_{51} = 105$, $a_{52} = 108, \ldots$ Find: ① Value of a_{200},

② Index where the term just is > 1000, and the previous term is < 1000

① General formula $a_n = a_1 + d(n-1)$

a_1: ? $\quad d$: $=3$ here

Now $a_{51} = 105 = a_1 + 3 \times 50 \Rightarrow a_1 = -45$

Next, $a_{200} = -45 + 3 \times 199$

$= 552$

② Find index $i \ni a_i > 1000$ and $a_{i-1} < 1000$

$a_i = a_1 + 3(i-1)$

$= -45 + 3i - 3$

$= \boxed{-48 + 3i > 1000}$

So, $3i > 1048 \Rightarrow i > \frac{1048}{3}$

$i = \left\lceil \frac{1048}{3} \right\rceil = 350$

Check $a_{349} = 999$, $a_{350} = 1002$

In geometric sequence the ratio between the term is constant.

Ex. Find the formula for a_n if the first few terms are: 1, 7, 25, 79, 241, 727, ...

Look at ratios $\frac{25}{7} = 3.57$ $\frac{79}{25} = 3.16$

$241/79 = 3.05$ $727/241 = 3.02$

ratio $\longrightarrow 3$

this means a_n is generated by formula having 3^n

n	1	2	3	4	5
3^n	3	9	27	81	243
a_n	1	7	25	79	241

· Formula $a_n = 3^n - 2$ for $n \geq 1$

$\therefore$ Formula $a_n = 3^n - 2$ for $n \geq 1$

So $a_7 = 3^7 - 2 = 2185$.

Aqil at 2/9/2021 8:04 AM

Summation

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + a_3 + \cdots + a_n$$

↑ index (always take integer values)

$$\sum_{i=1}^{n} c = c + c + \cdots + c = nc$$

$$\sum_{i=n}^{m} c = c(m - n + 1)$$

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{1}{2} n(n+1)$$

Proof Let $S = 1 + 2 + 3 + \cdots + n$ ($=n+1$, $=n+1$, $=n+1$, $=n+1$)

$$S = n + (n-1) + (n-2) + \cdots + 1$$

$$2S = n \times (n+1)$$

$\therefore S = \frac{1}{2} n(n+1)$

$1 + 2 + 3 + \cdots + (n-1) +$

$$\sum_{i=m}^{n} i = \underbrace{1+2+3+\cdots+(m-1)+}_{\sum_{i=1}^{n} i} \; m + (m+1) + (m+2) + \cdots + n \; \underbrace{- \left[1+2+3+\cdots+(m-1)\right]}_{\sum_{i=1}^{m-1} i}$$

$$= \frac{1}{2}n(n+1) - \frac{1}{2}(m-1)\times m$$

$$= \frac{1}{2}\left(n^2 + n - m^2 + m\right)$$

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + ar^3 + \cdots + ar^n$$

$$= a\left(\frac{r^{n+1} - 1}{r - 1}\right) \qquad r \neq 1$$

Proof.

Let $S = a + ar + ar^2 + \cdots + ar^n$

$rS = ar + ar^2 + ar^3 + \cdots + ar^{n+1}$

Subtract

$rS - S = ar^{n+1} - a$

$$\therefore S = \frac{a(r^{n+1} - 1)}{r - 1}$$

$$\sum_{i=m}^{n} ar^i = \sum_{i=0}^{n} ar^i - \sum_{i=0}^{m-1} ar^i$$

$$= a\left(\frac{r^{n+1} - 1}{r-1}\right) - a\left(\frac{r^m - 1}{r-1}\right)$$

$$= a\left(\frac{r^{n+1} - r^m}{r-1}\right)$$

Double summation $\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}$

$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} c\right)$ start with the innermost Σ $= \sum_{i=1}^{n} cm = cmn$

$= cm$

$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} i\right) = mi = \sum_{i=1}^{n} mi = \frac{1}{2}mn(n+1)$ (constant)

Consider $\sum_{i=1}^{n}\left(\sum_{j=i}^{m} i\right) = i(m - i + 1) = mi - i^2 + i$

$$= \sum_{i=1}^{n} (mi - i^2 + i)$$

$$= \sum_{i=1}^{n} (mi - i + 1)$$

$$= \underbrace{\sum_{i=1}^{n} mi} - \underbrace{\sum_{i=1}^{n} i^2} + \underbrace{\sum_{i=1}^{n} i}$$

$$= \frac{1}{2}mn(n+1) - \frac{n(n+1)(2n+1)}{6} + \frac{1}{2}n(n+1)$$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} j\right) = \frac{1}{2}m(m+1) = \frac{1}{2}nm(m+1)$$

Aqil at 2/11/2021 8:02 AM

Some other ways to express summations

$$\sum_{p \text{ prime} < 20} p = 2 + 3 + 5 + 7 + \cdots + 19$$

$$\sum_{k \text{ is odd integer between 5 and 30}} k = 5 + 7 + 9 + 11 + \cdots + 29$$

$$\prod_{i=1}^{n} c = c \times c \times \cdots \times c = c^n$$

$$\prod_{i=1}^{n} i = 1 \times 2 \times 3 \times \cdots \times n = n!$$

Proof Techniques

Each theorem takes the form "if p then q" $p \to q$

hypothesis فرضية — conclusion النتيجة

Proof methods: Induction, Counter examples, Direct proof, Indirect proof, proof by cases, proof by contradiction

① Direct Proof $p \to q$

Assume p is T proceed to show q is T

Prove "if n is odd (p), then n^2 is odd (q)".

Assume n is odd. Let $n = 2k+1$ for some integer k. Then

$$n^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2\underbrace{(2k^2+2k)}_{\text{integer}} + 1$$
$$= \text{odd}$$

② Indirect Proof $\neg q \to \neg p \iff p \to q$

② Indirect Proof $\neg q \to \neg p \iff p \to q$

Prove "if n^2 is odd (p) then n is odd (q)"

$\neg q$: Assume n is even. Let $n = 2k$. $k \in \mathbb{Z}$

Then $n^2 = (2k)^2 = 2(2k^2) = \text{even}$ $\neg p$

③ Proof by contradiction $\neg p \to F$

Show that $\sqrt{2}$ is irrational (p)

عدد غير كسري

$\neg p$: Assume $\sqrt{2}$ is rational.

Let $\sqrt{2} = a/b \ni a, b \in \mathbb{Z}$

a/b: Simplest form. No common factor.

Squaring $a^2 = 2b^2$ even $\Rightarrow$ a is even

Let $a = 2k$ $k \in \mathbb{Z}$

$\therefore a^2 = (2k)^2 = 2b^2$

$\Rightarrow b^2 = 2k^2$ even $\Rightarrow$ b is even

contradiction

Aqil at 2/14/2021 8:03 AM

In general, proof by contradiction

① $\neg p \rightarrow$ contradiction

② Assume $p \wedge \neg q$, use indirect proof $\neg q \rightarrow \neg p$, contradiction

Ex. Show that if $3n+2$ is odd (p) then n is odd (q)

Assume $3n+2$ is odd (p)

n " even ($\neg q$)

Now, n is even. Let $n = 2k$ for some $k \in \mathbb{Z}$.

$3n+2 = 3(2k)+2 = 2(3k+1) =$ even ($\neg p$) — contradiction

4] Proof by cases

To show $p \rightarrow q$ where $p = p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_n$

show $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$

Ex. Show that any integer ending with 2 cannot be a perfect square.

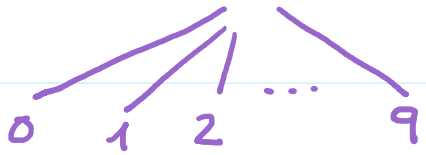
... 2

4, 9, 16, 25, 36, ...

Let n be an integer. We show n^2 cannot have 2 is units digit.

have 2 is units digit.

Let $n = 10k + \ell$



$n = 3659$, k, ℓ

$$n^2 = (10k + \ell)^2 = 100k^2 + 20k\ell + \ell^2$$
$$= 10(10k^2 + 2k\ell) + \ell^2$$

case 1 ($\ell = 0$). $\ell^2 = 0$

case 2 ($\ell = 1$). $\ell^2 = 1$

case 3 ($\ell = 2$). $\ell^2 = 4$

case 4 ($\ell = 3$). $\ell^2 = 9$

case 5 ($\ell = 4$). $\ell^2 = 16$

case 6 ($\ell = 5$). $\ell^2 = 25$

case 7 ($\ell = 6$). $\ell^2 = 36$

case 8 ($\ell = 7$). $\ell^2 = 49$

case 9 ($\ell = 8$). $\ell^2 = 64$

case 10 ($\ell = 9$). $\ell^2 = 81$

square of an integer ends with 0, 1, 4, 5, 6, 9

5 Counter example المثال المناقض

Ex. All prime integers are odd.

2 is even integer and is prime.

Aqil at 2/16/2021 8:07 AM

Mathematical Induction

Weak induction

Strong induction

Base case · P(1) is True

Inductive case

Assume $P(1) \wedge P(2) \wedge \cdots \wedge P(n) \rightarrow P(n+1)$

Base case P(1) is True

Inductive case Assume P(n) is True } $\forall n\ P(n)$

$P(n) \rightarrow P(n+1)$

Ex Use Induction to show $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

Let $P(n) =$ "$\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$"

Base case $(n=1)$

LHS $P(1) = \sum_{k=1}^{1} k = 1$

RHS $P(1) = \frac{1}{2} \times 1 \times 2 = 1$

$\therefore$ P(1) is True

Inductive case

Assume P(n) is True for some n. We show that P(n+1) is True.

$$\text{LHS } P(n+1) = \sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + (n+1)$$

$= \frac{1}{2}n(n+1)$ by induction hypothesis

$= \frac{1}{2}n(n+1) + (n+1)$

$$= (n+1)\left[\frac{n}{2} + 1\right]$$

$$= \frac{(n+1)(n+2)}{2}$$

$$= \text{RHS of } P(n+1)$$

Ex Use induction to show $\sum_{k=m}^{n} r^k = \frac{r^{n+1} - r^m}{r-1}$

Let $P(n) =$ " $\sum_{k=m}^{n} r^k = \frac{r^{n+1} - r^m}{r-1}$ "

Base case $(n = m)$

LHS of $P(m) = \sum_{k=m}^{m} r^k = r^m$

RHS of $P(m) = \frac{r^{m+1} - r^m}{r-1} = \frac{r^m(r-1)}{r-1} = r^m$

$\therefore$ $P(m)$ is True

Inductive case

Assume $P(n)$ is True. We show that $P(n+1)$ is True.

LHS of $P(n+1) = \sum_{k=m}^{n+1} r^k = \left(\sum_{k=m}^{n} r^k\right) + r^{n+1}$

$= \frac{r^{n+1} - r^m}{r-1}$ by induction hypothesis

$= r^{n+1} - r^m \quad r^{n+1}$

$$= \frac{r^{n+1} - r^m}{r-1} + r^{n+1}$$

$$= r^{n+1}\left(\underbrace{\frac{1}{r-1} + 1}_{= \frac{r}{r-1}}\right) - \frac{r^m}{r-1}$$

$$= \frac{r^{n+2}}{r-1} - \frac{r^m}{r-1}$$

$$= \frac{r^{n+2} - r^m}{r-1} = \text{RHS of } P(n+1)$$

Aqil at 2/21/2021 8:18 AM

Ex Let $H_k = 1 + 1/2 + 1/3 + 1/4 + \cdots + 1/k$

Show that $H_{2^n} \geq 1 + n/2$

$H_{2^n} = 1 + 1/2 + 1/3 + \cdots + 1/2^n$

Base case ($n = 0$)

LHS $= H_{2^0} = H_1 = 1$

RHS $= 1 + 0/2 = 1$

} is True

Inductive case

Assume H_{2^n} is true. We show it is true

Assume H_{2^n} is true. We show it is true for next n.

$$H_{2^{n+1}} = \boxed{1 + 1/2 + 1/3 + \cdots + \frac{1}{2^n}} + \underbrace{\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}}}$$

$\geq 1 + n/2$ by induction hypothesis

$\geq$ Smallest term $\times$ # terms $= 2^n$

Counting # terms $\frac{1}{2^n+1} + \cdots + \frac{1}{2^{n+1}}$

$$\Downarrow$$

$$\frac{1}{2^n+1} + \frac{1}{2^n+2} + \frac{1}{2^n+3} + \cdots + \frac{1}{2^n+2^n}$$

$$H_{2^{n+1}} \geq 1 + n/2 + \boxed{\frac{1}{2^{n+1}} \times 2^n} = 1/2$$

$$\geq 1 + \frac{n}{2} + \frac{1}{2} = 1 + \left(\frac{n+1}{2}\right)$$

Aqil at 2/23/2021 8:11 AM

Strong Induction

$$[P(1) \wedge P(2) \wedge \cdots \wedge P(n) \rightarrow P(n+1)] \rightarrow \forall n\, P(n)$$

Ex Show that any number $n \geq 8$ can be written as sum of 3s and 5s.

Let $P(n)$ = "n can be written as sum of 3s and 5s"

Base case ($n=8$)

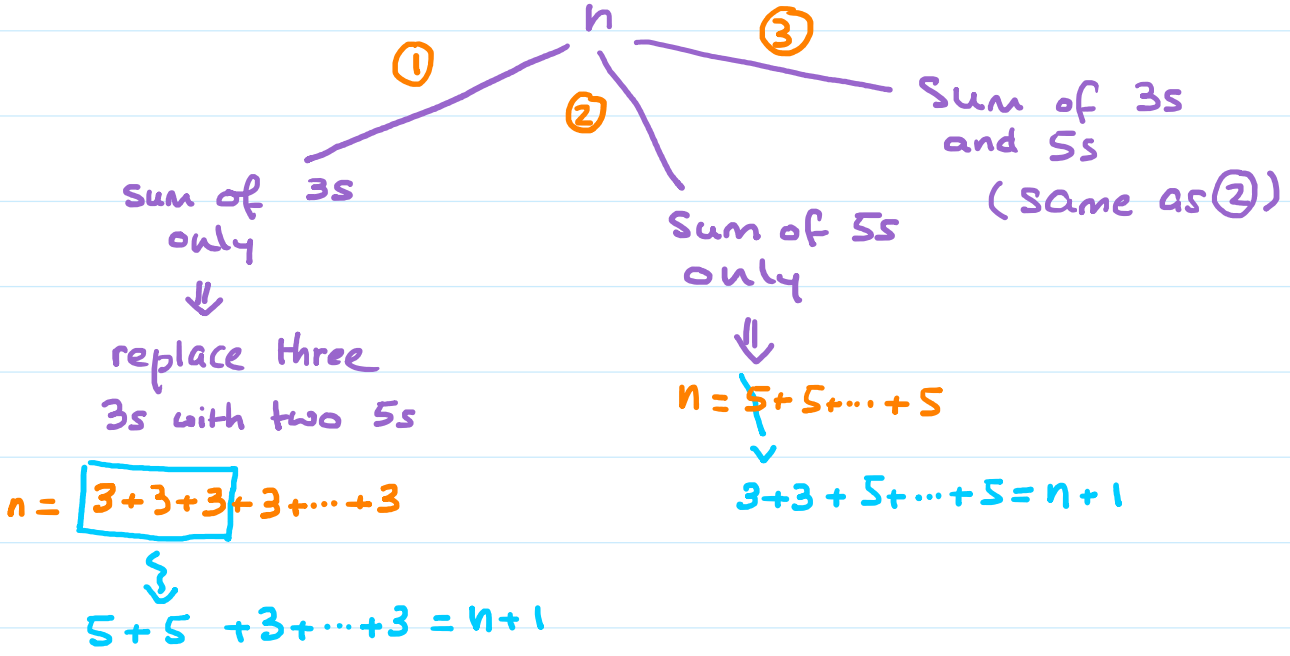
$8 = 3+5$. $P(8)$ is true.

Inductive case

Assume $P(k)$ is true for $k = 8, 9, 10, \ldots, n$.

We show $P(n+1)$ is true.

We have 3 cases.



Integers and Division

Def. integers a, b ∋ $a \neq 0$. Denote $a \mid b$ means a divides b.

b يقسم a

Also, $a \nmid b$ denotes a does not divides b.

Ex $3 \mid 9$, $5 \mid 25$, $6 \mid 12$

$3 \nmid 10$, $5 \nmid 16$, $6 \nmid 13$

Th integers a, b, c. Then

- if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$
- if $a \mid b$ then $a \mid bc$ ∀ any c
- if $a \mid b$ and $b \mid c$ then $a \mid c$

Proof. if $a \mid b$ then let $b = ax$ for some integer x.

Similarly $a \mid c$ then let $c = ay$ for some integer y.

$b + c = ax + ay = a(\underbrace{x+y}_{\text{integer}})$

therefore $a \mid (b+c)$

Def. A positive integer $p > 1$ is prime $\Leftrightarrow$ the only divisors are 1 and p.

NOTE: Not prime is called composite.

Ex. 7 is prime.

9 is composite since $3 \mid 9$

Th. Every positive integer can be written uniquely as product of primes.

Ex. $7 = 7$

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$1024 = 2^{10}$

Aqil at 2/28/2021 9:08 AM

Th. If n is composite then n has a prime divisor $\leq \sqrt{n}$

Proof

n composite $\Leftrightarrow n = ab \ni 1 < a \leq b < n$.

Now at any time either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

i.e can't have both a and $b > \sqrt{n}$ simultaneously

for it leads to $n = a \times b > \sqrt{n} \times \sqrt{n} = n$.

Ex. 102973 prime ?

Ex. 102973 prime ?

Try $2, 3, 5, 7, 11, \ldots, \lfloor \sqrt{102973} \rfloor = 320$

Ex. 109 prime ? $\lfloor \sqrt{109} \rfloor = 10$

$2 \nmid 109$, $3 \nmid 109$, $5 \nmid 109$, $7 \nmid 109$ $\Rightarrow$ 109 is prime.

Prime factorization : writing n as unique product of primes.

Ex. Find prime factors of $7007. = 7 \times 7 \times 11 \times 13$

$2 \nmid 7007$, $3 \nmid 7007$, $5 \nmid 7007$,

$7 \mid 7007 \Rightarrow \frac{7007}{7} = 1001$

$7 \mid 1001 \Rightarrow \frac{1001}{7} = 143$

$7 \nmid 143$

$11 \mid 143 \Rightarrow \frac{143}{11} = 13$

Ex. Find prime factors of $9761 = 43 \times 227$

$\lfloor \sqrt{9761} \rfloor = 98$

$2 \nmid 9761$, $3 \nmid 9761$, $5 \nmid 9761$, $7 \nmid 9761$

$11 \nmid 9761, \ldots, 41 \nmid 9761$,

$43 \mid 9761 \Rightarrow \frac{9761}{43} = 227 \Rightarrow$ Stop

my claim 227 is prime.

Because $43 > \sqrt{227}$. So if 227 was not

prime then we would had a prime divisor $\leq \sqrt{227}$.

Aqil at 3/2/2021 8:02 AM

Greatest Common Divisors & Least Common Multiple.

Def. a, b integers $\neq 0$.

The largest integer d ∋ $d \mid a$ and $d \mid b$ is called "greatest common divisor of a and b"

$\gcd(a, b)$ denotes the greatest common divisor of a, b.

Ex. Find $\gcd(24, 36) = 12$.

Divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24

" " 36: 1, 2, 3, 4, 6, 9, 12, 18, 36

Def. Integers a, b are relatively prime if $\gcd(a, b) = 1$.

Ex. $\gcd(12, 25) = 1$ so 12 and 25 are relatively prime.

Def. Integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1 \quad \forall\, i \neq j$

Ex. integers 10, 17, 21 are pairwise rel. prime

Since $\gcd(10, 17) = 1$

$\gcd(10, 21) = 1$

$\gcd(17, 21) = 1$

Ex. integers 10, 17, 22 are not pairwise rel. prime

Since $\gcd(10, 22) \neq 1$.

Let $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}$

$b = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n} = \prod_{i=1}^{n} p_i^{\beta_i}$

where $p_1, p_2, \ldots, p_n$ primes and $\alpha_i, \beta_i \geq 0$.

Then,

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \cdots \times p_n^{\min(\alpha_n, \beta_n)}$$

$$= \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$$

Proof. We show this is valid Formula for $\gcd(a, b)$

Let $d = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$, then

① $d \mid a$ and $d \mid b$ Since power of each prime does not exceed the power of this prime in either a or b.

② $\nexists\ d' > d \ni d' \mid a$ and $d' \mid b$.

This is due if we increase the power of any of the primes in d then either $d' \nmid a$ or $d' \nmid b$ or both.

Ex. Find $\gcd(120, 500)$

$$\left.\begin{aligned} 120 &= 2^3 \times 3 \times 5 \\ 500 &= 2^2 \times 5^3 \end{aligned}\right\} \gcd(120, 500) = 2^2 \times 3^0 \times 5^1 = 20$$

Def. The least common multiple of positive integers a, b is the smallest pos. integer which is divisible by both a, and b. Denoted $\operatorname{lcm}(a, b)$.

Given $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ $\quad b = \prod_{i=1}^{n} p_i^{\beta_i}$ $\quad \alpha_i, \beta_i \geq 0$

Then

$$\operatorname{lcm}(a, b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

Proof. Let $\gamma = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$

① Show $a \mid \gamma$ and $b \mid \gamma$

② Show $\nexists\ \gamma' < \gamma \ni a \mid \gamma'$ and $b \mid \gamma'$.

Ex. find $\operatorname{lcm}(120, 500)$

$120 = 2^3 \times 3 \times 5$

$500 = 2^2 \times 5^3$

$\operatorname{lcm}(120, 500) = 2^3 \times 3^1 \times 5^3$

$= 3000$

Th $a, b > 0$ integers. Then

$$a \times b = \gcd(a, b) \times \operatorname{lcm}(a, b)$$

Ex. $120 \times 500 = \gcd(120, 500) \times \operatorname{lcm}(120, 500)$

$= 20 \times 3000$

Modular Arithmetic

Def. integers a, $m > 0$. Let us denote the remainder of a/m by $a \bmod m$.

* $a \bmod m = r \quad \ni \quad a = mq + r$
  ↑ unique $\quad 0 \le r < m$

Ex $17 \bmod 5 = 2$

$-17 \bmod 5 = 3$ Since $-17 = 5 \times (-4) + 3$

Def. a, b, m integers, $m > 0$ then

$a \equiv b \bmod m \iff m \mid (a - b)$

↑ a is congruent to b modulo m

Ex. $17 \equiv 5 \mod 6$ Since $6 \mid (17 - 5)$

$20 \not\equiv 7 \mod 5$ " $5 \nmid (20 - 7)$

NOTE:

$a \equiv b \bmod m \iff a \bmod m = b \bmod m$

$a \not\equiv b \bmod m \iff a \bmod m \neq b \bmod m$.

Th Let $m > 0$ integer. Then

$a \equiv b \bmod m \iff \exists$ integer $k \ni a = b + km$

Proof. $\Rightarrow$

$a \equiv b \bmod m \Rightarrow m \mid (a-b)$

or $a - b = km$

$\therefore a = b + km$

$\Leftarrow$

Assume $a = b + km \Rightarrow a - b = km$

Hence $m \mid (a-b) \Rightarrow a \equiv b \bmod m$

Th Let $m > 0$ integer. if $a \equiv b \bmod m$ and $c \equiv d \bmod m$

Then, $a + c \equiv b + d \bmod m$

$a \times c \equiv b \times d \bmod m$

Proof.

$a \equiv b \bmod m \Rightarrow a = b + k_1 m$

$c = d \bmod m \Rightarrow c = d + k_2 m$

Then $a + c = b + d + (k_1 + k_2) \times m$

$(a + c) - (b + d) = (k_1 + k_2) \times m$

or $m \mid ((a+c) - (b+d))$

or $a + c \equiv b + d \bmod m$

Th Let $a = bq + r \ni a, b, q, r$ integers and $0 \le r < b$

Then

$\gcd(a, b) = \gcd(b, r)$

Proof.

if $d|a$ and $d|b$ then $d|(xa \pm yb) \ni x, y \in \mathbb{Z}$

Let $x = 1$, $y = q$,

then

$$d|(\underbrace{a - bq}_{= r}) \Rightarrow d|r$$

Meaning if $d|a$ and $d|b$ then $d|r$.

In other words, the common divisor of a, b, r is the same.

Applying above Theorem repeatedly we get the Euclidean algorithm for gcd.

Ex. Find gcd(287, 91) using Euclidean Algorithm

↝ must be ≥ 0 and < 91

$287 = \boxed{3} \times 91 + \boxed{14}$

$91 = \boxed{6} \times 14 + \boxed{7}$ $\Rightarrow$ our gcd

$14 = \boxed{2} \times 7 + \boxed{0}$

Recursive version of Euclidean Algorithm for gcd.

```
function gcd(a,b)                    // a ≥ b
{
    let r ∋ a = bq + r   and   0 ≤ r < b
    return r > 0 ? gcd(b,r) : b
```

}

Aqil at 3/9/2021 8:06 AM

Th if a, b positive integers then $\exists$ integers s and t $\ni$ $\gcd(a,b) = sa + tb$.

This means we can express gcd as a linear combination of its arguments.

Ex express $\gcd(252, 198)$ as linear combination of 252 and 198.

First use Euclidean Algorithm,

$252 = \boxed{1} \times 198 + \boxed{54}$

$198 = \boxed{3} \times 54 + \boxed{36}$

$54 = \boxed{1} \times 36 + \boxed{18}$ ⇐ gcd

$36 = \boxed{2} \times 18 + \boxed{0}$

$18 = 54 - 1 \times 36$

$= 54 - 1 \times (198 - 3 \times 54)$

$= -1 \times 198 + 4 \times 54$

$= -1 \times 198 + 4 \times (252 - 1 \times 198)$

$= 4 \times 252 - 5 \times 198$

$\therefore \gcd(252, 198) = 18 = 4 \times 252 - 5 \times 198$

Lemma a, b, c positive integers $\ni$ $\gcd(a,b) = 1$ and $a \mid bc$ then $a \mid c$.

Proof.

given $\gcd(a,b) = 1$

$= sa + tb$ (from Th.)

multiply both sides by c, then

$sac + tbc = c$

Now $a \mid sac$ and $a \mid tbc$ (given)

So,

$a \mid (\underbrace{sac + tbc}_{= c}) \Rightarrow a \mid c$

Lemma if p is prime and $p \mid a_1 \cdot a_2 \cdots a_n$ (all a_i are integers) then $p \mid a_i$ for some i

Th Let $m > 0$ integer, and a, b, c integers.

if $ac \equiv bc \mod m$ and $\gcd(c,m) = 1$

then $a \equiv b \mod m$.

Proof.

Given $ac \equiv bc \mod m \Rightarrow m \mid (ac - bc)$

$\Rightarrow m \mid c \times (a-b)$

But $m \nmid c$ since $\gcd(c,m) = 1$.

Therefore $m \mid (a-b)$ or $a \equiv b \mod m$

NOTE In general if $ac \equiv bc \mod m$ we can't cancel c from both sides unless $\gcd(c,m) = 1$.

Consider $7 \times 2 \equiv 5 \times 2 \mod 4 \Rightarrow 7 \equiv 5 \mod 4$

~~from~~ ~~unless~~ ~~gcd(a,m) = 1.~~

Consider $7 \times 2 \equiv 5 \times 2 \mod 4 \Rightarrow 7 \equiv 5 \mod 4$

it is wrong to cancel 2 here since $\gcd(2,4) \neq 1$.

Th if a, m are relatively prime then $\exists$ a unique integer $\acute{a} < m \Rightarrow a \times \acute{a} \equiv 1 \mod m$.

$\acute{a}$ ↑ inverse of a modulo m

Proof.

Given $\gcd(a,m) = 1 \Rightarrow sa + tm = 1$

$sa + tm \equiv 1 \mod m$

but $m \mid tm \Rightarrow sa \equiv 1 \mod m$

s ↑ is the inverse of a in modulo m which we called $\acute{a}$

Ex Find inverse of 4 in modulo 7

Since $\gcd(4,7) = 1$ so $\exists$ inverse of 4 in modulo 7.

$2 \times 4 = 8 \equiv 1 \mod 7 \Rightarrow 2$ is the inverse of 4

Aqil at 3/11/2021 8:05 AM

Since 7 is prime so all numbers have inverse.

no.	1	2	3	4	5	6
inverse	1	4	5	2	3	6

Ex. construct inverse table for numbers modulo 8

No.	1	2	3	4	5	6	7

inverse 1 — 3 — 5 — 7

↑ no inverse since 2 and 8 are not relatively prime.

Ex What is the inverse of 19 in modulo 59

19 and 59 are relatively prime ⇒ inverse ∃

① Write gcd of 19 and 59 using Euclidean

② express gcd as linear combination

$59 = \boxed{3} \times 19 + \boxed{2}$

$19 = \boxed{9} \times 2 + \boxed{1} = \gcd$ ↑

$1 = 19 - 9 \times 2$

$= 19 - 9 \times (59 - 3 \times 19)$

$= -9 \times 59 + 28 \times 19$

inverse

∴ inverse of 19 is 28

Check $19 \times 28 = 532 \equiv 1 \mod 59$

Ex Solve equation $22x \equiv 3 \mod 51$

Do we have a unique solution? yes since 22 and 51 are relatively prime.

$x \equiv 3 \times$ (inverse of 22 in modulo 51) $\mod 51$

Euclidean gcd(51, 22)

Write gcd as linear combination

$x \equiv 3 \times 7 \mod 51$

$\equiv 21 \mod 51$

General solution $x = 21 + 51k \quad k \in \mathbb{Z}$

Ex Solve $4x^2 \equiv 3 \mod 9$

4 and 9 are relatively prime so we may have either two solutions or no solution

$x^2 \equiv 3x$ (inverse of 4 in modulo 9) $\mod 9$

$\equiv 3 \times 7 \mod 9$

$\equiv 3 \mod 9$

x	x^2	$x^2 \mod 9$	
1	1	1	} no value = 3
2	4	4	
3	9	0	
4	16	7	
5	25	7	
6	36	0	
7	49	4	
8	64	1	

Thus there is no solution

Th Chinese Remainder Theorem (CRT)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime.

then $x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$\vdots$

$x \equiv a_n \mod m_n$

has a unique solution modulo $m = m_1 \times m_2 \times \cdots \times m_n$.

The solution x is $\ni$ $0 \le x < m$.

Aqil at 3/14/2021 8:03 AM

Ex. Solve

$x \equiv 2 \mod 3$ ($a_1 = 2$, $m_1 = 3$)

$x \equiv 3 \mod 5$ ($a_2 = 3$)

$x \equiv 2 \mod 7$ ($a_3 = 2$, $m_3 = 7$)

} are pairwise relatively prime

Let $m = m_1 \cdot m_2 \cdot m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{m}{m_1} = 35$ $\quad M_2 = \frac{m}{m_2} = 21$ $\quad M_3 = \frac{m}{m_3} = 15$

Solution $x = a_1 \cdot M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \mod m$

y_1: inverse of M_1 in modulo m_1

i.e $M_1 y_1 \equiv 1 \mod m_1$

Find y_1. $35y_1 \equiv 1 \mod 3 \Rightarrow y_1 = 2$

" y_2. $21y_2 \equiv 1 \mod 5 \Rightarrow y_2 = 1$

" y_3. $15y_3 \equiv 1 \mod 7 \Rightarrow y_3 = 1$

$\therefore x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \mod 105$

$= 23$

General Solution $x = 23 + 105k \quad \ni \quad k \in \mathbb{Z}$

Th Fermat's Little Theorem

Th **Fermat's Little Theorem**

If p prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$

or, $a^p \equiv a \bmod p$.

NOTE: the converse is not true.

Ex. According to Fermat $6^{10} = 60466176 \equiv 1 \bmod 11$

$7^{10} \equiv 1 \bmod 11$

How to calculate $a^k \bmod p$ quickly ?

Ex calculate $15^{100} \bmod 31 = ?$

According to Fermat $15^{30} \equiv 1 \bmod 31$

$(15^{30})^3 = 15^{90} \equiv 1^3 \bmod 31$

$\therefore 15^{100} \bmod 31 = 15^{90} \times 15^{10} \bmod 31$ ($15^{90} \equiv 1$)

$\equiv 15^{10} \bmod 31$

$15^1 \equiv 15 \bmod 31$

$15^2 = 225 \equiv 8 \bmod 31$

$15^4 = (15^2)^2 \equiv 8^2 \bmod 31 \equiv 2 \bmod 31$

$15^8 \equiv 2^2 \bmod 31 \equiv 4 \bmod 31$

$\therefore 15^{10} = 15^8 \times 15^2$

$\equiv 4 \times 8 \bmod 31$

$\equiv 1 \bmod 31$

So $15^{100} \equiv 1 \mod 31$

Th Euler's Generalization

If a and n are relatively prime,

then,

$$a^{\phi(n)} \equiv 1 \mod n,$$

where $\phi(n)$ is Euler's totient function

= # of numbers $< n$ that are relatively prime to n.

$$\phi(n) = |\{x \mid 1 \le x < n \text{ and } \gcd(x,n) = 1\}|$$

$$= n \prod_{p|n} \left(\frac{p-1}{p}\right) \qquad p \text{ is prime } < n$$

Ex $\phi(12) = |\{1,5,7,11\}| = 4$

$\phi(15) = |\{1,2,4,7,8,11,13,14\}| = 8$

Aqil at 3/16/2021 8:08 AM

$12 = 2^2 \times 3, \quad \phi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$

$15 = 3 \times 5, \quad \phi(15) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$

note if p prime then $\phi(p) = p-1$.

Let $n = p$ in Euler. $a^{p-1} \equiv 1 \mod p$ (Fermat)

Ex What is the last two digits of 27^{1203}

$27^{1203} = \ldots\ldots XX$ ← last two digits

digits = 1722

Last two digits $= 27^{1203} \bmod 100$.

Can't use Fermat since 100 not prime.

Euler, $\phi(100) = 40$

$27 \bmod 100$

according to Euler $27^{40} \equiv 1 \bmod 100$

$27^{1203} = (27^{40})^{30} \times 27^{3} \bmod 100$, $(27^{40})^{30} \equiv 1$

$\therefore 27^{1203} \bmod 100 \equiv 27^{3} \bmod 100 = 83$

Public Key Cryptosystem

cancel eath other

P_A S_A — A ——— B — P_B S_B

C

P_B public key (known by all)

S_B secure key (do not share)

① Secure messaging m

A sends to B $P_B(m)$

B reads message $S_B(P_B(m)) = m$

② Authentication توثيق

A sends to B $S_A(P_B(m))$

B reads message $S_B(P_A(S_A(P_B(m)))) = m$

RSA

1. Pick two large primes p, q
2. Let $n = p \times q$
3. Pick public key e $\ni$ $\gcd(e, (p-1)\times(q-1)) = 1$
4. Compute secure key d $\ni$ $de \equiv 1 \mod (p-1)(q-1)$

M = original message

C = Cipher text

then, $C = M^e \mod n$ encryption

$M = C^d \mod n$ decryption

Aqil Azmi at 3/23/2021 8:03 AM

Ex. Let $p = 43$, $q = 59$

$n = p \times q = 2537$

Pick $e = 13$, note $\gcd(13, \underbrace{42\times58}_{=2436}) = 1$

Compute d $\ni$ $13d \equiv 1 \mod 2436$

Using Euclidean we get $937 \times \underbrace{13}_{e} - 5 \times 2436 = 1$
$\underbrace{\quad\quad}_{d}$

M_1 M_2

M = "ST|OP" (letter → number A = 00, B = 01, ...)

1819 1415

M = SI OF (letter → number A = 00, B = 01, ...)

1819 1415

$C_1 = M_1^e \bmod n = 1819^{13} \bmod 2537 = 2081$

$C_2 = M_2^e \bmod n = 1415^{13} \bmod 2537 = 2182$

Recover the message

$M_1 = C_1^d \bmod n = 2081^{937} \bmod 2537 = 1819$

$M_2 = C_2^d \bmod n = 2182^{937} \bmod 2537 = 1415$

Combinatorics

Basic counting principles

Sum rule

Do task T_1 or T_2 (not both)

$\#\text{ways} = |T_1| + |T_2|$

$|T_1|$: #ways to do task T_1

Product rule

Do tasks T_1 and T_2

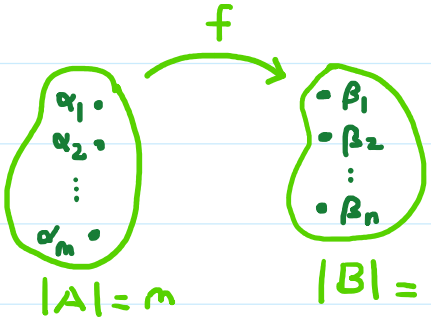
$\#\text{ways} = |T_1| \times |T_2|$

Ex

Sum rule: pick one item only from either box A or box B = $n + m$ choices

Product rule: Pick one item only from each box = $n \times m$ choices

Ex How many functions are there from a set with m elements to a set with n elements.



each of the $\alpha \in A$ has n choices

α_1 has n choices

α_2 " n "

.

$|A| = m$ $|B| = n$ a_2 " n "

$\vdots$

a_m " n choices

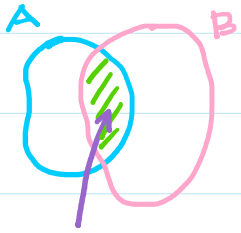
Product rule $\Rightarrow$ n^m functions

Aqil Azmi at 3/25/2021 8:10 AM

Principle of inclusion-exclusion

overcounting $\Rightarrow$ remove these elements

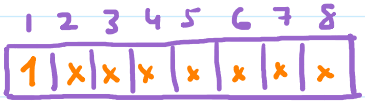
undercounting $\Rightarrow$ add " "



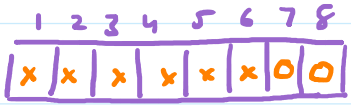
counted twice

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Ex How many bit strings of length 8 either start w/a 1 bit or ends w/two 00



or



Can have $2^7 = 128$

can have $2^6 = 64$ patterns

this pattern counted twice

$2^5 = 32$ patterns

bitstrings $= 128 + 64 - 32 = 160$

bitstrings = 128 + 64 − 32 = 160

Pigeonhole Principles

Th if $k+1$ or more objects are placed into k boxes then there is at least one box with two or more objects.

Proof. Suppose each box has one object ⇒ total # objects is at most k. A contradiction since we have $k+1$ objects.

Ex Class with 13 students ⇒ two or more students must be born in same month.

Th Generalized Pigeonhole

If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

Proof.

Recall $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1 \quad \forall x \in \mathbb{R}$

$$\# \text{objects} \leq k \times (\lceil N/k \rceil - 1)$$

$$< k \times (((N/k) + 1) - 1) = N$$

This contradicts the # objects $= N$

Ex This class has 38 students. Then there are at least $\lceil 38/12 \rceil = 4$ who were born in same month

least $\lceil 38/12 \rceil = 4$ who were born in same month

Ex Suppose we have 10 black, 10 white, 10 red and 10 brown socks. All mixed up. How many to pick so to guarantee two of same color.

= Pick Smallest $N \ni \lceil N/4 \rceil = 2$ ← want two of same color

↑ # colors

$\Rightarrow N = 5$

How many socks to pick up so we have 2 red.

Pick 32 socks.

Worst case scenario: 1st 10 are all black

2nd " " " white

3rd " " " brown

Aqil Azmi at 3/30/2021 8:04 AM

Ex Given set of numbers: 1, 2, 3, ..., 25. Pick any 14.

Show that there are at least two numbers who sums 26.

1 2 3 . . . 11 12 13

25 24 23 . . . . 15 14

26 26 26 26 26

We have 12 pairs that sum 26.

Pick 14. Worst scenario we pick 1, 2, ..., 13. The 14th will be one of 14, ..., 25 and it will pair with one of the numbers to sum 26.

with one of the numbers to sum 26.

Permutation & Combination

Def. Permutation of set of distinct objects is an ordered arrangements of these objects.

Th # of r-permutations of n distinct elements is

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

Def. The r-combination of a set is an unordered selection of r element from set

Th # of r-Combination of a set with n distinct elements $(0 \le r \le n)$ is

$$C(n,r) = \binom{n}{r} = \frac{n!}{r! \cdot (n-r)!}$$

Ex Count # bit strings of length = 10 that has exactly 3 zeros.

$= \binom{10}{3}$ order does not matter as we are picking 3 zeros.

Ex Count # bit strings of length = 10 that has at least 3 zeros.

$\binom{10}{} \quad \binom{10}{} \cdots + \binom{10}{} = \sum^{10} \binom{10}{}$

least 3 zeros.

$$= \binom{10}{3} + \binom{10}{4} + \cdots + \binom{10}{10} = \sum_{k=3}^{10} \binom{10}{k}$$

Ex. How many ways to arrange 10 books $= 10!$

Ex. Suppose we have 4 books in Arabic (A)
3 " " Math (M)
3 " " CS (C)

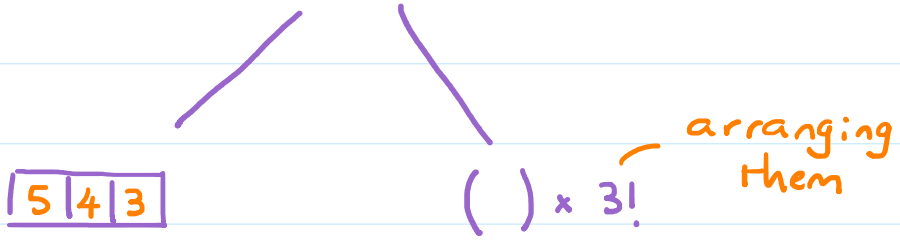
How to many ways to arrange if we want one subject books together.

$$= 3! \times 4! \times 3! \times 3!$$

- $3!$: # ways to arrange by subject (AMC, ACM, ⋮, CMA)
- $4!$: #ways to arrange Arabic books
- $3!$: #ways to arrange math books
- $3!$: #ways to arrange CS books

Aqil Azmi at 4/1/2021 8:03 AM

Ex 5 People. How many ways to photograph them in groups of 3.



5	4	3

$P(5,3)$

$(\ ) \times 3!$ them

Selecting 3 out of 5

Ex Suppose out of these 5 one person must be in each picture

1	4	3

$\times 3$

$P(4,2) \cdot \binom{3}{1}$

↑ where to place the must picture person

Selecting 2 out of 4

$\binom{4}{2} \times 3!$

↑ arranging them

Ex Computer password of length 6 .. 8 characters.
Characters are either lowercase letter or numeral.
Each password must have at least one digit.

passwords $= P_6 + P_7 + P_8$

P_6 = # of password of length 6 with 1 digit

\+ # " " " " " " 2 digits

⋮

\+ # " " " " 6 with 6 digits

places to put the digit

10	26	26	26	26	26

$\times 6$

$$= \binom{6}{1} \times 10 \times 26^5 + \binom{6}{2} \times 10^2 \times 26^4 + \cdots + \binom{6}{6} \times 10^6$$

↑ one digit; 10^2: 2 digits; 26^4: 4 letters

places to put digit

$$= \sum_{k=1}^{6} \binom{6}{k} \times 10^{k} \times 26^{6-k} = 36^{6} - 26^{6}$$

(no restriction; only letter)

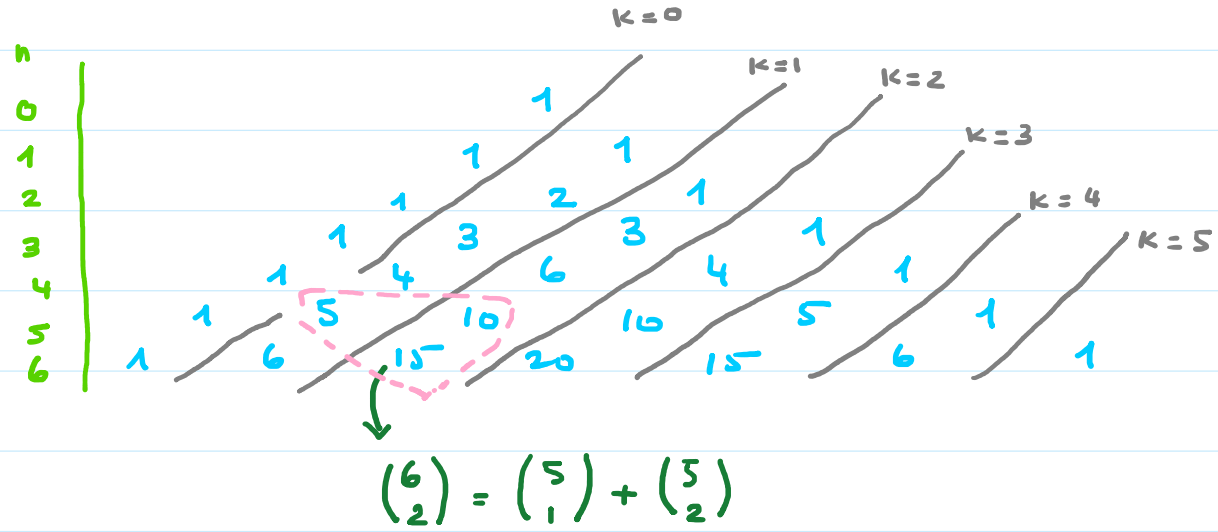
Similarly P_7 and P_8

$$\#\text{ passwords} = \sum_{n=6}^{8} \sum_{k=1}^{n} \binom{n}{k} \times 10^{k} \times 26^{n-k}$$

Binomial Coefficient

Th Pascal's identity: let $n, k \in \mathbb{Z}^+$ with $n \geq k$ then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$



$$\binom{6}{2} = \binom{5}{1} + \binom{5}{2}$$

Aqil Azmi at 4/6/2021 8:03 AM

Th Binomial Theorem

Let $x, y \in \mathbb{R}$ and $n \in \mathbb{Z}^+$ then

$$(x+y)^n = \sum^{n} \binom{n}{k} x^k \cdot y^{n-k} = \sum^{n} \binom{n}{k} x^{n-k} \cdot y^k$$

Let $x, y \in \mathbb{R}$ and $n \in \mathbb{Z}$ then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \cdot y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} \cdot y^k$$

$$= x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} \cdot y^2 + \cdots + y^n$$

Ex $(x+y)^2 = \sum_{k=0}^{2} \binom{2}{k} x^k \cdot y^{2-k} = y^2 + 2xy + x^2$

Ex $(x+y)^4 = \sum_{k=0}^{4} \binom{4}{k} x^{4-k} \cdot y^k$

$= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

Th Let n be positive integer, then $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Proof. In Binomial Th. let $x = y = 1$

Th. Let $n \in \mathbb{Z}^+$ then $\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} = 0$

Proof. In Binomial Th. let $x = 1$, $y = -1$

Th Vandermonde's Identity

Let $m, n, r \in \mathbb{N}$ with $r \leq \min(n, m)$. Then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \cdot \binom{n}{k}$$

Corollary $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

Proof. Use Vandermonde's identity with $m = n = r$.

And $\binom{n}{k} = \binom{n}{n-k}$

Ex Find coeff of x^{12} in $(3x - 5/x^2)^{30}$

$$(3x - 5/x^2)^{30} = \sum_{k=0}^{30} \binom{30}{k} \cdot \underbrace{(3x)^k \cdot (-5/x^2)^{30-k}}$$

$$3^k \cdot x^k \cdot (-5)^{30-k} \cdot (x^{-2})^{30-k}$$

$$= 3^k \cdot (-5)^{30-k} \cdot x^{k-60+2k}$$

$$= 3^k \cdot (-5)^{30-k} \cdot x^{3k-60}$$

we want $3k - 60 = 12 \Rightarrow k = 24$

coeff of $x^{12} = \binom{30}{24} \cdot 3^{24} \cdot (-5)^6$

Th Multinomial theorem

If $n \in \mathbb{Z}^+$, then

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1+n_2+\cdots+n_k=n} c(n; n_1, n_2, \cdots, n_k) \cdot x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}$$

such that $c(n; n_1, n_2, \ldots, n_k) = \dfrac{n!}{n_1! \cdot n_2! \cdots n_k!}$

In short

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1+n_2+\cdots+n_k=n} \frac{n!}{n_1! \cdot n_2! \cdots n_k!} \cdot \prod_{i=1}^{k} x_i^{n_i}$$

Ex Find expansion of $(x + y + z)^2$

$$(x + y + z)^2 = \sum \frac{2!}{\quad} \cdot x^a \cdot y^b \cdot z^c$$

$$(x+y+z)^2 = \sum_{a+b+c=2} \frac{2!}{a!\cdot b!\cdot c!}\cdot x^a\cdot y^b\cdot z^c$$

a	b	c	
0	0	2	$= z^2$
0	1	1	$= 2yz$
0	2	0	$= y^2$
1	0	1	$= 2xz$
1	1	0	$= 2xy$
2	0	0	$= x^2$

$$\therefore (x+y+z)^2 = x^2 + 2xy + 2xz + y^2 + 2yz + z^2$$

Aqil Azmi at 4/8/2021 8:09 AM

Generalized Permutation and Combination

* r-permutation: select r objects out of n such that order matters.

w/o repetition: $P(n,r) = \frac{n!}{(n-r)!}$

w/ repetition: n^r

Ex # words of length 5 formed from English alphabet

26	26	26	26	26

$\therefore$ # of words $= 26^5$

* r-Combination: pick any r objects out of n such that order not important

w/o repetition

w/rep.

w/o repetition

$$\binom{n}{r} = \frac{n!}{r! \cdot (n-r)!}$$

w/rep.

$$\binom{n+r-1}{r} \quad \exists\ r \geq 0$$

Ex. 10 apples, 10 oranges, 10 bananas.

Pick 2 different fruits $= \binom{3}{2} = 3$

Pick any 2 fruits $= \binom{3+2-1}{2} = \binom{4}{2} = 6$

Ex. How many integer solutions does the eq.

$x + y + z = 11$ have $\exists\ x, y, z \geq 0$.

Solutions corresponds to # ways of selecting 11 (fruits) from 3 different types of fruits.

Solutions $= \binom{3+11-1}{11} = \binom{13}{11} = 78$

Ex. Suppose we want $x+y+z = 11$ $\exists$ $x \geq 1$, $y \geq 2$, $z \geq 4$.

How many solutions?

$n = 3$. Total $1+2+4 = 7$. # remaining $= 11 - 7 = 4$.

We want # solutions of $x+y+z = 4$ $\exists\ x, y, z \geq 0$.

Solutions $= \binom{3+4-1}{4} = \binom{6}{4} = 15$.

check

Oranges	Apples	Banana
1	2	8
1	3	7
1	4	6
1	5	5
1	6	4

2	2	7
2	3	6
2	4	5
2	5	4
3	2	6
3	3	5
3	4	4
4	2	5
4	3	4
5	2	4

Ex. Find # solutions to $5 \le x+y+z \le 11 \quad \exists\, x,y,z \ge 0$

$=$ # solutions of $x+y+z=5$

$+$ # " " $x+y+z=6$

$\vdots$

$+$ # " " $x+y+z=11$

$$= \sum_{r=5}^{11} \binom{3+r-1}{r}$$

Permutations with indistinguishable objects

Ex. How many different strings can we write by re-arranging letters of SUCCESS

$n=7$

$n = 7$ (# letters)

$$\#\text{ strings} = \frac{n!}{n_c! \cdot n_s!} = \frac{7!}{2! \cdot 3!}$$

$2!$: # C's, $3!$: # S's

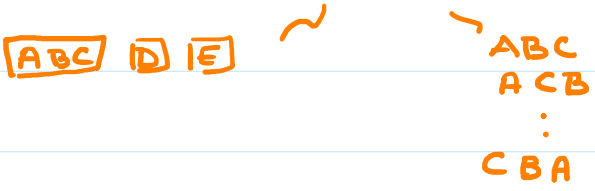
Aqil Azmi at 4/11/2021 10:02 AM

Ex Consider the letters: A, B, C, D, E.

1. # words of length = 5 (duplicate letters allowed) = 5^5
2. # words " " = 4 (dup. allowed) = 5^4
3. # words of length = 5 (each letter once) = $5!$
4. # " " " = 4 (each letter once) = $P(5,4)$
5. # " " " = 3 (each letter once) = $P(5,3)$

6. # words of length = 5 (each letter once) and A, B together = $4! \times 2!$

7. # words of length = 5 (each letter once) and the letters A, B not together = $5! - 4! \times 2!$
8. # words of length = 5 (each letter once) and the letters A, B, C together = $3! \times 3!$



Ex Count # integers between 1 and 100 that are divisible by 6.

Numbers divisible are: 6, 12, 18, 24, ...

these are $6K$ $(K \geq 1)$. Want $6K \leq 100$

$\therefore K = \left\lfloor \frac{100}{6} \right\rfloor = 16$

Ex Count # integers between 1 and 100 that are divisible by 12 and 18.

Ex Count # integers between 1 and 100 that are divisible by 12 and 18.

Smallest integer that is divisibly by 12 and 18 = lcm(12,18)

$\therefore$ count $= \left\lfloor \frac{100}{\text{lcm}(12,18)} \right\rfloor = 2$ Check: 36, 72

Ex Count # integers between 1 and 100 that are divisible by 12 or 18.

= # of those divisible by 12

+ # " " " " 18

− # of those common to 12 and 18.

$= \left\lfloor \frac{100}{12} \right\rfloor + \left\lfloor \frac{100}{18} \right\rfloor - \left\lfloor \frac{100}{\text{lcm}(12,18)} \right\rfloor = 11$

Ex Count # integers between 150 and 500 that are divisible by 12 or 18.

= Count those between 1 .. 500

− Count those between 1 .. 149

$= \left\lfloor \frac{500}{12} \right\rfloor + \left\lfloor \frac{500}{18} \right\rfloor - \left\lfloor \frac{500}{\text{lcm}(12,18)} \right\rfloor$

$- \left(\left\lfloor \frac{149}{12} \right\rfloor + \left\lfloor \frac{149}{18} \right\rfloor - \left\lfloor \frac{149}{\text{lcm}(12,18)} \right\rfloor \right)$

نهاية المنهج - والحمد لله رب العالمين